NEMZETBIZTONSÁGI SZEMLE
9. évfolyam (2021) 2. szám 81–94. • DOI: 10.32561/nsz.2021.2.6

Molnár Tamás József[1]

Az internetes biztonság és az OSINT összefüggései

Correlation between Internet Security and OSINT

Az OSINT (Open Source Intelligence) mozaikszó mint a nyílt forrású hírszerzés jelentősége az elmúlt években egyre nagyobb szerepet kap az egyes szolgálatok életében, hiszen a digitális információk megszerzése és birtoklása új kihívások elé állítja a szakembereket. A legtöbben biztosan hallottuk már azt a közhelyet, miszerint „ami egyszer felkerül az internetre, az ott is marad". Ezt szem előtt tartva kell mindennapi munkánkat végeznünk, hiszen soha nem tudhatjuk, hogy ki és mikor használhat fel ellenünk olyan személyes információkat, amelyek megszerzéséhez mi magunk szolgáltattuk az adatokat valamikor a közel- vagy régmúltban.

Jelen írásban az OSINT jelenetőségének bemutatását követően a digitális tudatosság fontosságát hangsúlyozva rámutatok néhány tipikus gyenge pontra, úgymint a gyermekek és az idősebb korosztály e téren hiányos ismeretei, az operációs rendszerek, más programok adatgyűjtései, a kiszivárgott vagy gyűjtött adatbázisok jelentette veszélyek, az adatvesztés körülményei és következményei. Kitérek továbbá az egyre bővülő speciális adatgyűjtő célszoftverekre is. Ezek kapcsán megoldási javaslatokat vázolok fel, amelyek hasznos segítséget jelenthetnek akár a prevenciót, akár a veszteségek minimalizálását illetően.

Kulcsszavak: *Digitális Öntudatosság, információbiztonság, digitális lábnyomok, OSINT, adatvédelem, prevenció*

The importance of Open Source Intelligence (OSINT) is getting a bigger role in the lives of services in recent years, because the acquiring and possessing of digital information poses new challenges for professionals. Most of us have probably heard the commonplace that 'once something posted on the Internet it stays there forever'. We have to do our daily job with this in mind, as we never know who and when can use personal information against us, for which we have provided the data ourselves

[1] Molnár Tamás József gazdasági informatikus, kommunikátor, igazságügyi IT-szakértő. E-mail: tamas.j.molnar@gmail.com

at some point in the recent or distant past. As a part of this article, I present the importance of the OSINT and while underlining the importance of digital awareness, I point out some typical weaknesses, such as the lack of knowledge of children and the elder age group in this field, the data collection of operating systems and other programs. The dangers posed by leaked or collected databases and circumstances and consequences of data loss, I also cover the continuously expanding field of special data collection software. Based on these, I outline a solution proposal that can be a useful help in terms of either prevention or minimisation of losses.

Keywords: *digital consciousness, information security, digital footprints, OSINT, data protection, prevention*

1. Bevezető – OSINT a mindennapokban

OSINT. Mit is jelent ez a pár betű, ez a napjainkban sokat látott mozaikszó? Egyre többször kerül elő mind szakmai körökben, mind az interneten böngészve az Open Source Intelligence kifejezés rövidebb formája. Aki még nem hallott róla, annak is első helyen dobja a Wikipédia a böngészőnkbe beütve. De valójában miről van szó? Pár szóban megfogalmazva: az emberi hanyagságról, a kényelmességről, a nemtörődömségről, az internet végeláthatatlan hálózatában információként magunk után hagyott digitális lábnyomainkról, amelyek aztán nyílt forrásokból összegyűjtve tovább elemezhetővé válnak.

Meglehetősen nehéz szavak ezek, és joggal merülhet fel az olvasóban, hogy miért lenne ez így probléma, hiszen Ő mindenről tud, amit az interneten intéz, használ, vagy csak böngészik. Egyrészről valóban tehetjük mindezt körültekintően és elővigyázatosan, de jobb, ha tudjuk, hogy teljesen láthatatlanok jóformán nem lehetünk a digitális világban, és ezt a kiberbűnözők is pontosan tudják. Nagyon sok támpontot meg kell vizsgálnunk ahhoz, hogy elérjünk az OSINT valódi lényegéhez, ahol olyan nyílt információkat tudunk összegyűjteni egy személyről vagy csoportról, amelyeket vagy saját maga (esetleg barátai, ismerősei) hagyott hátra, vagy a családja oszt meg róla, esetleg ellopták róla azok, akiknek feladatuk az információszerzés. Az információszerzés célcsoportja maga az ember és az információkat tároló egységek, a számítógépek és az információtechnológiai hálózatok.

A kommunikációelméletekben az információcsere alapszabályai szerint annak létrejöttéhez minimum két fél szükséges, akiket adónak és vevőnek hívunk, a köztük lévő információt segítő közeg a csatorna, illetve lehetnek közben zavaró tényezők, amelyek vagy zavarják a kommunikációt vagy lehetetlenné teszik azt. Az információkat tudjuk kódolni és dekódolni – amennyiben arra van szükségünk, hogy más ne értse a két fél közötti információáramlást –, de itt is lehetnek váratlan tényezők, amelyek közbeszólnak, akadályozzák vagy ellehetetlenítik a kommunikációt. Amennyiben az információcsere rendben lezajlik a felek között, a következő megvizsgálandó probléma abból adódik, hogy lehetett-e olyan harmadik fél a folyamat lezajlása alatt, aki hozzájutott az adatokhoz, miközben erre mi magunk nem adtunk engedélyt. Itt megint több csoportra tudjuk bontani a kérdést, hiszen vannak olyan jól ismert tényezők

és nemzetbiztonsági kérdések, amikor szükség van azokra az adatokra, amelyek a felek között keletkeznek, de a mostani témakörben nem ezekkel a kérdésekkel fogunk foglalkozni. Előfordulhatnak olyan esetek is, amikor nem tudunk róla, hogy az adataink más érdekeltségek kezébe jutnak és ezeket az adatokat összegyűjtve hatalmas adatbázisokban tárolva gyűjtik, esetleg eladják olyan csoportoknak vagy cégeknek, akik ezekből az információkból profitálni tudnak.

Az OSINT-tevékenység lényege tehát, hogy olyan tartalmakat kutassunk fel a hírközlő és továbbító hálózatok segítségével, amely tartalmakat nyílt forrásokból, legális eszközökkel gyűjtünk össze, rendszerezzük azokat és elemző-értékelő munkafolyamatokat végzünk rajtuk a további feldolgozhatóság érdekében.

De honnan és hogyan tudunk ilyen információkat szerezni? Milyen módszereket tudunk bevetni annak érdekében, hogy információhoz jussunk egy adott személyről vagy csoportról? A válasz sok esetben megdöbbentően egyszerű és gyors folyamatot takar, amibe egy laikus ember bele sem gondol. A probléma megértéséhez a bevezető elején leírt pár szóhoz kell visszakanyarodnunk, ahol azt fogalmazom meg, hogy emberi hanyagság vagy lustaság generálja a munkánk valódi mibenlétét. Hiszen biztosan ismerünk olyan embert, aki úgy állítja be jelszavát a számítógépén, hogy saját születési adataival kezdi a begépelést, esetleg a gyermeke nevét hozzágépelve, vagy kedvence becenevét használva változtatja meg az utálatos havi jelszóváltoztatás üzenet után a hitelesítő adatot. Biztos vagyok benne, hogy mindenki hallott már olyan emberről, aki a jelszavát esetleg felírja egy cetlire és ezt a monitorjára ragasztja, hogy ne felejtse el, vagy a jól bevált 1234567 után még hozzátesz egy nyolcadik számot a számsorhoz. Esetleg ismerünk olyan kollégát, aki kedvenc autómárkáját pötyögi be rendületlenül a jelszóváltoztató téglalapba azt gondolva, hogy ily módon szuperbiztonságos lesz a rendszere, és védve vannak a legfontosabb privát vagy irodai adatai az illetéktelenek elől. Talán hallottunk már olyan esetről is, ahol a telefon PIN-kódja 1234, vagy 0000; esetleg olyanról is, aki teljes egészében kiiktatja ezt a lehetőséget, mert naponta 30 alkalommal kellene használni.

Azok számára, akik azt gondolják, hogy ezzel a hozzáállással soha nem fognak semmilyen adatszivárgást elszenvedni, szomorú hírem van: valószínűleg már túl is vannak rajta! Erre azonban abban az esetben is nagy az esély, ha a kor követelményeinek megfelelően olyan jelszót választanak a szociálismédia-profilnak, vagy e-mail-címnek, ahol odafigyelnek a kis- és nagybetű kombinációra, esetleg számmal vagy speciális karakterrel kiegészítve adnak biztosnak hitt jelszót maguknak.

A 2019-es évben felfedezett majd 2020-ban berobbant, Covid-19 okozta világjárvány nemcsak a társadalmi, egészségügyi és gazdasági problémákról lesz nevezetes a történelemkönyvekben, hanem a kibertámadások eddig sohasem látott aranykoraként is emlegetni fogják majd a következő generációk. Az információkereskedelem olyan mértéket ölt napjainkban, hogy nem is lehet kiszámolni, nagyságrendileg mekkora mennyiségű kiszivárgott adat kerül ki minden nap a digitális térbe, hiszen egy meghatározó hányadukra csak akkor derül fény, amikor már közzétették azokat, és a hackerek erre szakosodott fórumokon árulják – sok esetben pár dollárért vagy euróért.

Ezekből az adatokból olyan információkat lehet leszűrni, amelyek segítségével a legtöbb esetben olyan mennyiségű és minőségű adat válik egy konkrét személyhez köthetővé, amivel egy számunkra ismeretlen emberről akár egy teljes profilt létre

tudunk hozni. Mindezt olyan, nyílt információkból szerzett adatokból, amelyeket könnyedén össze tudunk gyűjteni az internetről, vagy nyíltan beszerezhető és letölthető formában, vagy speciálisan erre a szakágra létrehozott célszoftverek segítségével kutathatók ki.

Nem titkolt tény a nyílt információszerzés körében, hogy a közösségi profilok terjedésével kezdett el egyre nagyobb érdeklődés mutatkozni a személyes információk gyűjtése iránt, hiszen a ma már jóformán mindenki által használt szociálisháló-profilokból rengeteg adat gyűjthető össze, deríthető ki bárkiről. Az IOT- (*Internet of Things* – Dolgok Internete)[2] eszközök forradalmasították a digitális otthonok kényelmi szintjét, és az úgynevezett „okoseszközeink" további sérülékenységi pontokat adnak az adatszivárgásoknak, ha nem megfelelően vannak beállítva, vagy a már említett biztonsági és hitelesítési kódolásaik nem érik el a megfelelő szintet.

Ezek az eszközök mind regisztrációhoz kötöttek, ahol meg kell adnunk a személyes adatainkat, hitelesítő kódjainkat, e-mail-címünket vagy telefonszámunkat. Ezekkel a regisztráció során elkért/megadott személyes azonosítókkal olyan információkat adunk ki a kezünkből, amelyekkel egy személy beazonosítását teljes mértékig véghez lehet vinni, és egy konkrét emberhez lehet kötni.

2. OSINT – múlt, jelen, jövő

„A nyílt forrású információszerzés (Open Source Intelligence, továbbiakban OSINT) olyan információgyűjtő eljárás, amelynek során a nyilvánosan elérhető forrásokból az információkat felkutatják, elemzik, értékelik és felhasználják egy adott cél érdekében. Az OSINT nem egyenlő az Internetről, a közösségi média eszközeiből szerzett információgyűjtéssel, mint ahogy ebből következően nem az elmúlt évtizedek új eljárása. A hagyományos (nyomtatott és elektronikus) média, szürke irodalom, szakértők és megfigyelők tapasztalatai, kereskedelmi műholdas felvételek, könyvtárak anyagai, tanulmányok, nyilvános konferenciák előadásai, de prospektusok, reklámanyagok mind-mind részét képezhették a nyílt forrású információgyűjtésnek. Ez egyben azt is jelenti, hogy ezt a hírszerző eljárást nem csak a nemzetbiztonsági szolgálatok végzik, hanem a politikai, üzleti, civil szférában egyaránt alkalmazzák."[3]

Tagadhatatlan tehát, hogy a nyílt információszerzés nem az internet terjedésével kezdődött, hanem sokkal régebben, hiszen az emberi kíváncsiságot és információéhséget mindig is ki kellett elégíteni, így maga a tevékenység sokkal régebbre vezethető vissza, mint azt gondolnánk. Az írás és az olvasás, valamint a nyomtatott könyvek és a sajtó terjedésével egyszerűbb lett az adatok megszerzése, kategorizálása és begyűjtése, és ez kétséget kizáróan a digitális hálózatok és az internet terjedésével lett egy robbanásszerűen elterjedt folyamat, ami a gyors információcserék segítségével egyre dinamikusan fejlődő iparággá növi ki magát.

---

[2] Benedek Gergő: *Mi is az az IOT? És mi az AIOT? Minden, amit a dolgok internetéről tudni kell.* (2020. február 12.).

[3] Bányász Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe. *Nemzetbiztonsági Szemle,* 3. (2015), 2. 21–36.

Gondoljunk csak bele, a millenium környékén, amikor még a legtöbb háztartásban betárcsázós internetet használtunk külső modemmel, amikor a TV-antennánk belföldi, földfelszíni analóg adást fogott, és mobiltelefonunkkal egy-két soros megjelenítésen tudtunk rövid üzeneteket küldeni egymásnak. Vagy amikor a 2001-es népszámlálás során bemondás alapján, papíralapon töltötte ki a számlálóbiztos a felvett adatokat – sokkal kisebb volt a beáramlott adatok mennyisége, nem beszélve a hibalehetőségekről, elveszett adatokról és a lassú feldolgozásról. Statisztikákat alap irodai szoftverekkel tudtunk készíteni, ami a legtöbb esetben betáplált adatok alapján szép kör- vagy oszlopdiagrammokat jelentett, jobb esetben már színes nyomtatóval kiprintelt lapok sokaságát. A prezentációkat a feletteseinknek a meetingeken (akkoriban megbeszélésnek mondtuk) átlátszó celofán lapokra írtuk és rajzoltuk, amit a technikai szobából előhúzott írásvetítőn tudtunk bemutatni a csoportnak.

Ezeket olvasva: ugye, mennyit fejlődtünk csupán 21 év alatt? Ma már az óvodás gyermekünk napi étkeztetését reggelente a mobilunk segítségével hagyjuk jóvá, a garázsban a gépkocsinkat távolról indítjuk be, hogy meleg és kellemes legyen beleülni az induláskor, a mobiltelefonunk családtag lett – hiszen sok esetben többet foglalkozunk vele, mint a családtagjaink problémáival –, távolról indítjuk be a klímánkat vagy bármilyen elektromos eszközünket a digitális otthonunk rendszerének segítségével. Otthonról dolgozunk, hiszen a home office létjogosultsága sosem volt ennyire egyértelmű és bizonyított, nagyobb gyermekeink digitális oktatásban részesülnek, a lejáró személyes okmányaink intézése céljából otthonról foglalunk időpontot az okmányirodába, és még sorolhatnánk naphosszat, hogy mi mindent tudunk elintézni a technikai hálózatok és IOT-eszközök segítségével. És ezek mögött a hálózatok és eszközök mögött mind-mind egy digitális másunk, illetve avatárunk van regisztrálva, rengeteg adattal és személyes információval.

Mivel ezeket az adatokat digitálisan tárolják és az ezeket feldolgozó számítógépek csak előre betáplált programok alapján működnek, nem lehet kizárni az adatvesztés és az adatlopás lehetőségeit, ám ezekkel részletesebben később fogunk foglalkozni. A személyes adatok nyilvánossá tétele sokkal nagyobb kihívást jelent bárki számára, hiszen sok esetben bele sem gondolunk abba, hogy burkoltan vagy különböző csalásokkal és megtévesztő módszerekkel olyan információkat tudnak kicsalni tőlünk, amelyekkel a bűnözők szó szerint el tudják lopni a digitális másunkat, hatalmas károkat okozva ezzel mind a személyünknek (banki visszaélések, csalások), mind a gazdasági vagy állami érdekek területén (például Covid-19-vakcina-információk beszerzése a gyártóktól).[4]

A nyílt információk megszerzése a jövőben további kihívásokat fog majd jelenteni a szakmának, de a trend már most egyre világosabban látszik: egyrészt a személyes információk megszerzése különböző legális módszerekkel egyre nagyobb kapacitásokat fog igényelni (adatok tárolása, feldolgozása), másrészt a szociális média térhódítása, valamint a digitális eszközök és újabb technológiák megjelenése egyre több és nagyobb adatmennyiség feldolgozásával fog járni, mind informatikai mind humán kapacitás tekintetében.

[4] Jessica Davis: Hackers Leak COVID-19 Vaccine Data Stolen During EU Regulator Breach. *Health IT Security,* 2021. január 13.

3. Digitális tudatosság

A digitális öntudatosság az a magatartás, amit minden olyan felelős embernek, aki digitális eszközt vagy internetet használ, követnie kell; amivel a személyes adatait megvédi, tudatosan magáról a legkevesebb információt jelenít meg nyíltan, és ezeket az információkat folyamatosan karbantartja, aktualizálja saját maga vagy olyan személy érdekében, aki azt nem képes megtenni a környezetében.

Meg kell említenünk azt a tényt is, hogy a kiberbűnözők módszerei is egyre kifinomultabbak az információk megszerzését illetően, hiszen ők is egyre jobban idomulnak az információtechnológia fejlődő lehetőségeihez – kihasználva ezekkel azokat az emberi tulajdonságokat, amelyekre hatva megszerzik azokat a kulcsfontosságú adatokat, amelyekkel át tudják venni az irányítást akár az életünk felett is. A másik tényezőről mi magunk tehetünk: ezzel olyan információkat szivárogtatunk ki egyenesen a bűnözőknek, amelyekkel tálcán kínáljuk a lehetőséget a bűncselekmények elkövetéséhez.

Egy egyszerű példa segítségével szeretném szemléltetni, hogy milyen könnyen tudunk csapdába esni a saját figyelmetlenségünk miatt. Az utóbbi időben hatalmasat nőtt az úgynevezett SIM swap[5] csalással elkövetett bűncselekmények száma. Az első lépcsőben nyílt információszerzéssel a közösségi oldalakat böngészve olyan leendő áldozatokat keresnek a támadók, ahol a kiszemeltek közzéteszik (kiposztolják) utazásaikat, drága, újonnan megvásárolt értéktárgyaikat. Sok esetben még a boltokat és helyszíneket is megjelöli az áldozat („becsekkol"), ezzel már a vásárlás helyét és idejét elárulva információt ad az eseményről. Közösségi oldalára kiposztolt képekből szintén helyszíneket lehet azonosítani, illetve a képek exif adataiból[6] ismét „értékes" információkat tehetünk közzé. A közösségi oldalakon megjelenített, vagy az oldalra regisztrált e-mail-címek és telefonszámok segítségével már közvetlenebbül meg tudják szólítani az áldozatot további csalási módszerek segítségével, ami lehet adathalászat e-mail-cím felhasználásával, vagy egyszerű marketingalapú megkeresés/adatszerzés, esetleg hivatalos vagy ügyintéző személy képében történő adatnyerés. A nyílt interneten rengeteg olyan adatbázis kering, amelyekből kiszivárgott banki információkon át az összes adatunkat meg lehet tudni (felhasználóneveinket, számlavezető bankunk nevét, a folyószámlaszámunkat vagy éppen édesanyánk nevét, lakcímünket, személyazonosító okmányaink számát), és ezeket az adatbázisokat akár ingyen is be tudjuk szerezni.

A SIM swap[7] csalásban az a legijesztőbb, hogy a bűnöző és az áldozat között semmilyen kontaktus nem szükséges, sőt még a telefonkészülékünk sem kell ahhoz, hogy tovább tudjanak lépni. A csalók a megszerzett adatok segítségével felveszik a kapcsolatot az áldozat telefonszolgáltatójával, és miután hitelesítették magukat, a megszerzett adatokkal új SIM-kártyát igényelnek (jellemzően azzal az indokkal, hogy azonnal kell nekik vagy lopás miatt, vagy kisebb méretű SIM-kártyával működő új készülék beszerzése okán). Ezáltal az áldozat SIM-kártyáját deaktiválva az új SIM-kártyára

[5] Perei Dóra: Hogyan védekezhetünk a SIM-csere átverés ellen? *Rakéta,* 2021. január 11.
[6] Tips & Tricks – Tech: *Nézd meg az EXIF metaadatokat iPhone, Android, Mac és Windows rendszeren.* (é. n.)
[7] Jason Cipriani: SIM swap fraud: How to prevent your phone number from being stolen. *Cnet,* 2020. szeptember 29.

terhelve már a bűnöző telefonjára érkeznek az üzenetek. Mivel telefonszámunk sok esetben a második autentikációs eszközünk,[8] a jelszavaink, azonosító adataink kinyerése után arra is tudjuk használni, hogy visszaállítsuk jelszavunkat, vagy belépjünk vele a netbankunkba, e-mailünkbe vagy közösségimédia-profilunkba.

Összességében tehát megállapítható az, hogy a digitális tudatosság igenis fontos része kell legyen a felelős internethasználatnak: annyira kell védeni személyes adatainkat, jelszavainkat, mint egyéb ingó vagy ingatlan értékeinket.

4. A gyermekek és az idősebb korosztály felkészítése az internet előnyeire és veszélyeire, prevenciós intézkedések

Egy újabb nagyon fontos témakör azokkal a célcsoportokkal foglalkozni, amelyek a legsebezhetőbbek a kibertér világában, akiknek nincsen kellő tudásuk/tapasztalatuk az internet világát illetően még, vagy már nem tudnak kellően felelősen gondolkozni: ezek pedig a legfiatalabb és a legidősebb korosztály.

Elsőként a gyermekekre ható, célzott, tudatos reklámok, reklámkampányok, valamint a szociális média hatásait kell megemlíteni. Rögtön a gyermek első éveiben már mobiltelefonokat adunk kezükbe, tableten vagy egyéb digitális eszközön futtatjuk nekik az applikációkat, bekapcsoljuk a YouTube-csatornákat, ahol olyan digitális tartalmakhoz férhetünk hozzá, amelyekkel a kicsiket akár órákra a képernyő elé tudjuk kötni. Mobilunk segítségével applikáción keresztül indítjuk el az okos fogkefét, vagy a bluetooth-kapcsolaton keresztül csatlakozó okos játékokat az appok segítségével irányítjuk.

Természetesen ezekhez az alkalmazásokhoz is regisztrálnunk kell egy szerverre: a legtöbb esetben egy közel-keleti szolgáltatóhoz, amely ezeket az adatokat különböző adatbázisokban tárolva sok esetben nem a legbiztonságosabb módon menti el a felhő tárhelyeken vagy saját szerverein. Ezek az adatok legtöbbször nem tartalmaznak olyan információkat, amelyekből közvetlenül egy személyhez köthetünk egy profilt, azonban ezeket és sok más kiszivárgott, egyéb adatbázist összefésülve már igen valós és veszélyes kombinációkat vagy profilokat lehet létrehozni. Később, ahogy a gyermek növekszik, átveszi a jól ismert, gyermekek körében terjedő trendeket, létrehoz digitális profilokat, közösségi média avatárokat, Facebook, Instagram, Twitter, TikTok, Fun-fact, WhatsApp stb. regisztrációkat. Még később Skype, Viber, Snapchat, Pinterest, LinkedIn, Tinder, QQ, WeChat, Telegram, Signal stb. profilokat létrehozva ezeken keresztül hatalmas mennyiségű adatot szivárogtat ki magáról és a környezetéről úgy, hogy nem is gondolná, mekkora veszélynek teszi ki magát közben. Hiszen egy nyitott, nyilvános profil beállításánál nagyon sok oldalt nemcsak az ismerősök látnak, hanem szinte bárki.

Érdemes megfigyelni a napi posztok során, hogy a környezeti háttér, egy otthonról kiposztolt üzenet alkalmával milyen információkat tudunk legyűjteni csupán

[8] Pőcze Balázs: Öt mondatban: mi az a kétfaktoros autentikáció, és miért jó nekem? *Rakéta,* 2019. november 12.

a lakáskörülményeket figyelembe véve. A háttérben megbúvó hatalmas LCD-tv, a szülők féltve őrzött tárgyai, a lakás riasztórendszer-érzékelőinek elhelyezkedése (esetleg feltételezhető hiánya) egyaránt árulkodó. A festményeket a falakon, az asztalon hagyott ékszereket, laptopokat vagy számítógépeket, és sorolhatnánk, hogy mi mindent tudunk megfigyelni egy kellő körültekintés nélkül az interneten kiposztolt kép alapján. Mindezek megfigyelésére, kiszűrésére már készültek speciális szoftverek, amelyek különböző felismerő algoritmusokkal figyelik ezeket a háttérben megbúvó, apróságnak számító, de értékes tárgyakat, vagy a környezet biztonságosságát, illetve annak ellenkezőjét, hogy hova lehetséges kevés kockázattal, sikeresen betörni.

Természetesen OSINT-szempontból is nagyon értékesek ezek az információk, hiszen a legyűjtött multimédiás kép- és videóanyagokat kiszűrve egyre gyorsabban körvonalazódik egy személy kreált vagy valódi profilja.

Kötelesek vagyunk tehát felhívni a gyermekeink figyelmét, hogy egyrészről kellemes és „trendi" dolog használni a közösségi média nyújtotta előnyöket, de arra is figyelmeztetnünk kell őket, hogy megannyi veszély leselkedik rájuk olyan forrásokból, amelyekre nem is gondolnak. Ha időben elkezdjük a digitális öntudatosságot beléjük nevelni és elmagyarázzuk a problémák mibenlétét, nagyobb eséllyel tudjuk ösztönözni a következő generációkat azoknak a biztonsági módszereknek az alkalmazására, amelyekkel meg tudják védeni a privát szférájukat, és ezzel megelőzhetünk sok olyan jövőbeni bűncselekményt is, amelyek kihatással lehetnek a mindennapi életünkre, munkánkra és szociális kapcsolatainkra.

A gyermekek után az idősebb korosztály védelme a következő témakör, amivel foglalkoznunk kell. Míg a gyermekek játszva megtanulják a digitális eszközök használatát, az idősebb generációk számára komoly nehézséget, kihívást jelenthet egy-egy eszköz használata. Természetesen vannak erre nagyon is fogékony emberek, de a statisztikákat nézve annak a korosztálynak a tagjai, akik még nem használtak olyan okos eszközt, ami manapság már mindennapos az életünkben, nagyon nehéz és kihívásokkal teli feladat lehet akár elmagyarázni is ezeknek az elektronikus eszközöknek a mindennapi használatát.

Szinte mindenki hallott az „unokázós csalásról" és az ehhez az elkövetési körhöz fűződő bűncselekményekről, ahol az idősebb embereket telefonon felkeresi a csaló, hogy egy hozzátartozójának kiadva magát pénzt csaljon ki az áldozattól. Általában ezeket a hívásokat is olyan telefonhívások előzik meg, ahol a bűnözők akár statisztikai/közvéleménykutatási céllal álcázva olyan célzott, de nem feltűnő kérdéseket tesznek fel, amelyekből rengeteg információt tudhatnak meg egy idős emberről és környezetéről. Majd később ezeket az adatokat felhasználva csalnak ki pénzt vagy egyéb értéket az áldozatoktól. Az idősebb generációk internethasználatával kapcsolatban is vannak olyan veszélyek, amikor kémprogramokkal, célzott információkkal, reklámokkal vagy e-mailen terjedő kártevőkkel fertőzik meg a számítógépeket, amelyeken keresztül az operációs rendszer sérülékenységeit vagy a hiszékeny személy nem kellő hozzáértését kihasználva adatokat lopnak el, vagy adatokat gyűjtenek a felhasználó beleegyezése és tudta nélkül.

Megoldási javaslatok:

- Használjuk otthoni hálózatunkban a „szülői felügyelet” opciót, ahol szűrni lehet a gyermekünk eszközén a megjeleníthető tartalmakat. Ugyanitt időzíteni is tudjuk az internet elérhetőségét, időtartamokra lebontva.
- Beszéljük meg és magyarázzuk el gyermekünknek az internet nyújtotta előnyöket, és hívjuk fel a veszélyeire is a figyelmet.[9]
- Állítsunk be vírusirtó, tűzfal és malware szűrő programokat a digitális eszközökre.
- Előfizetéses opcióknál (például YouTube prémium) le tudjuk tiltani a reklámokat a videók közt, lejátszási listákat tudunk létrehozni, sőt, legálisan tölthetjük le a tartalmakat offline használathoz.
- Az idősebb korosztály védelmében szintén állítsunk be erős jelszavakat, vírusírtót és esetleg távoli asztali elérhetőséget biztosító programot, amivel távolról is tudunk segíteni egy esetleges problémánál.

5. Operációs rendszerek, programok adatgyűjtése, GDPR

Kaptunk már olyan üzenetet a számítógépen, amiben egy program vagy applikáció engedélyt kért tőlünk, adataink személyesebbé tételéhez? Webböngészőnkben hagytunk már jóvá úgynevezett cookie-kat engedélyező vagy tiltó üzenetet? Kellett már „adatvédelmi nyilatkozatot” kipipálnunk egy program telepítésénél? Amennyiben használunk számítógépet vagy digitális eszközt, valamelyik kérdésre a válasz biztosan igen. Természetesen a legtöbb felhasználó nem olvassa el azt a mellékelt, sok esetben 20–30 oldalas tájékoztatót, amiben pontosan szabályozva van az Európai Irányelv szerinti GDPR *(General Data Protection Regulation),*[10] azaz az általános adatvédelmi rendelet szerinti szabályzat, miszerint milyen személyes adatokat gyűjthetnek rólunk a felhasználó által kiválasztott cégek. A GDPR gyakorlatilag mindenkire vonatkozik, minden vállalatra vagy egyéb szervezetre, aminek minimum egy fő alkalmazottja vagy legalább egy ügyfele, kapcsolata van.

A közismert informatikai nagyvállalatok, mint például a jól ismert Microsoft, amelyeknek az operációs rendszereit használjuk szerte a világon és a hazai kormányzatban, a közigazgatásban és a vállalati szektor döntő részénél, illetve a legtöbb háztartásban is, külön adatvédelmi tájékoztatókat készítenek a felhasználók számára, és a rendszereik használata előtt külön kitöltendő űrlapokon kell jóváhagyni az általuk használni kívánt szoftver adatkezelési szabályait. Természetesen dönthetünk úgy is, hogy nem fogadjuk el ezeket, viszont ezek a szabályok nem keverendők össze az általános szerződési feltételekkel *(Terms and conditions),* amelyek a szoftver használatával kapcsolatos szabályokat és a használati feltételeket rögzítik.

Az informatikai vállalatok gyűjthetik a felhasználói adatokat a „felhasználói élmény növelése” érdekében, és ezek az adatok rengeteg olyan információt tartalmaznak

[9] Lica: Kémprogramokkal ellenőrzik a gyerek netezését. *Index.hu,* 2013. május 5.

[10] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) A természetes személyeknek és személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (EGT-vonatkozású szöveg).

a szoftvert használóról, amelyekkel célzottan tudják manipulálni vagy rávenni a fogyasztót, hogy több terméket használjon vagy vásároljon.

Rengeteg panasz érkezett a szoftverfelügyelethez a célzott reklámok miatt, illetve sok olyan esetet is regisztráltak, amikor arról panaszkodtak bizonyos szoftvert vagy közösségi oldalt használók, hogy csak beszéltek egy témával kapcsolatban, és ezután célzottan olyan reklámok jelentek meg az internetes felületeiken, amelyek a témához kapcsolódnak.[11]

Megoldási javaslatok:

- Az operációs rendszerünkben az adatvédelemnél (Windows start/gépház/adatvédelem) ki tudunk kapcsolni minden olyan funkciót, amelyek adatot gyűjtenek és továbbítanak rólunk.
- Böngészési előzményeinket rendszeresen töröljük a Shift+Ctrl+Del gombok lenyomása után. Használjunk inkognitó módot, ha érzékeny tartalmakat nézünk. Chrome: címsávtól jobbra – inkognitólap. Firefox: címsávtól jobbra – új privát ablak.
- A mentett oldalak előzményeit és beállításait célprogrammal, például Ccleanerrel tudjuk törölni vagy optimalizálni.
- Sose használjunk nyílt wifihálózatokat, ahol nem kérnek hitelesítést az ügyintézéseink céljából.

6. Kiszivárgott vagy gyűjtött adatbázisok és azok OSINT-jellegű felhasználása

A nyílt információjú adatszerzés egyik legnagyobb port kavaró esete a 2020-as év szeptemberében elhíresült OKIDB vagy másnéven Zhenhua Data Leak[12] volt, ami abból az okból kapott nagy nyilvánosságot, hogy sok magyar közszereplő és politikus nyílt információkból megszerzett adatait tartalmazta; mint utólag kiderült, a megszerzett adatok közt az egész világon található összes nemzet szerepelt mint potenciálisan megfigyelt cégekről és személyekről összegyűjtött adatbázis.

Természetesen nem ez volt az első ilyen adatszivárgás, illetve adathalmaz-gyűjtemény, ami ráébresztette a kiberbiztonsági szakértőket arra, hogy nyílt forrású adatokból mekkora terjedelmű és milyen minőségű adatokat lehet találni az interneten, amelyek ráadásul bárki számára elérhetőek és nem is kell speciális szakértelem hozzájuk (például a darknet ismerete), ezek nélkül is kis kutatómunkával megtalálhatók és letölthetők. Manapság a megfelelő fórumokon a kiberbűnözők, kezdő hackerek akár pár euró összegért hozzáférhetővé teszik ezeket az adatbázisokat, tehát már nem is arról van szó, hogy hatalmas aktákban több százezer nevet vagy címet és személyes adatot kell kicsempészni bárhonnan. Ehelyett egy körömnyi, 512 Mbyte nagyságú

[11] Bodnár Zsolt: Csak kiejted a szádon, hogy „üdítő", és már jön is szembe a neten a kólahirdetés. Mi folyik itt? *Qubit,* 2018. augusztus 21.

[12] Daniel Hurst – Lily Kuo – Charlotte Graham-McLay: Zhenhua Data Leak: personal details of millions around world gathered by China tech company. *The Guardian,* 2020. szeptember 14.

microSD kártyára letöltött anyagból egy egész nagyvállalat összes adatát, kutatási eredményeit vagy dolgozóinak a személyes adatait, belépési kódjait el tudják tulajdonítani, vagy a neten keresztül le tudják tölteni bárhol a világon, ha nincs megfelelő védelem ezek mögött a rendszerek mögött.

Vehetjük azonban azt a példát is, amikor olyan szerverek adatait sikerül megszerezniük a támadóknak, ahova mi magunk regisztrálunk fel a hivatalos, vállalati vagy privát e-mail-címünkkel. Ezeknél az eseteknél a megcélzott cég szervereinek sérülékenységét, nem naprakész állapotát használják ki a támadók, és ebben az esetben is nagyon érzékeny adatokat, e-mail-címeket, jelszavakat tudnak megszerezni. A legutóbbi adatszivárgás 2021 februárjában látott napvilágot, ahol a leírások szerint közel 3,2 milliárd e-mail-jelszó párosítás került ki az internetre. A COMB (*Compilation of Many Breaches*[13]) -ként elhíresült adatszivárgás csak egy a több tízezer kiszivárgott adatbázis közül, és ezeknek a száma naponta emelkedik több száz esettel. Mivel ezeket az adatokat könnyen meg lehet találni az interneten, az OSINT-munkamenetben a következő évek legnagyobb adatszerzési trendjéről beszélhetünk, hiszen ezek között az adatok között bárki keresgélhet kedvére.

Megoldási javaslatok:

- Több esetben felhívták rá a figyelmet, és folyamatosan figyelik a kiszivárgott e-mail-jelszó párokat, adatbázisokat a szakemberek. Megoldásként mi magunk is ellenőrizhetjük saját e-mail-címünket, hogy a kiszivárgott listákon szerepelünk-e. Amennyiben a beírt cím után pirosra vált az állapotsor, célszerű azonnal jelszót cserélni az érintett postafiókon.[14]
- Jelszavunkat olyan módon válasszuk meg, hogy speciális karaktert is tartalmazzon, kis és nagybetű kombinációjával, számokkal, valamint ne utaljon ránk (név, becenév, születési idő) semmilyen körülmények közt. Esetleg használhatunk komplett mondatokat.
- Használjunk másodlagos autentikációs eszközt, kétfaktoros hitelesítést, kulcsgenerátort vagy jelszómenedzser-programot.
- Ne használjunk mindenhová egy jelszót, és időközönként változtassuk meg azt. Mobil eszközeinken használjunk ujjlenyomat-ellenőrző vagy arcfelismerő funkciót.

7. Adataink elvesztése

Akár hagyományos papíralapú adatokról, dokumentumokról, akár digitális adatról legyen szó, amiket kezdetben floppylemezeken, CD-n, DVD-n és manapság már memóriakártyán, pendrive-on vagy bármilyen egyéb digitális adathordozón tároltunk/tárolunk, nagy körültekintéssel és odafigyeléssel kellett és kell kezelni, hogy ne kerüljön illetéktelenek kezébe olyan információ, amivel visszaélést, illetve bűncselekményt lehet elkövetni.

[13] Bernard Meyer: COMB: largest breach of all time leaked online with 3.2 billion records. *Cybernews,* 2021. február 12.

[14] ,; –have i been pwned?: https://haveibeenpwned.com/; *Check if your data has been leaked*: https://cybernews.com/personal-data-leak-check/

Az iratkezelési szabályzatok régen is pontosan meghatározták a papíralapú adatok tárolásának vagy megsemmisítésének folyamatát (azaz egy dokumentum lapjai nem összegyűrve, szemétkosárban végzik, hanem speciálisan erre rendszeresített iratmegsemmisítőben), és manapság is nagyon fontos betartani ezeket a szabályokat a digitális adatokra vonatkozóan. A fontosságukat tekintve ugyanolyan lényeges betartani és védeni adatainkat, hiszen, ha egy pendrive-ra másoljuk az irodai munkánkat – ráadásul titkosítás nélkül –, amelyet azután egy szerencsétlen véletlen következtében elvesztünk vagy ellopnak tőlünk, súlyos következményekkel járhat bárki számára mind erkölcsi, anyagi, mind büntetőjogi értelemben.

Abban az esetben, amikor már nincs szükség az adat további megtartására, a hordozható eszközről törölnünk kell azt, de nem egyszerű törléssel, hanem az úgynevezett wipe-olás (azaz speciális programmal történő többszörös adatterület-felülírás) technikájával. A sima törlés egy adathordozó, mobil eszköz tekintetében jóformán semmit sem számít, hiszen amíg az adott adatterület nincs felülírva, speciális szoftverek segítségével bármikor visszaállítható és kinyerhető a töröltnek gondolt információ. Ezért kiemelkedően fontos, hogy bármilyen adatunk is legyen, azoknak a védelme, kezelése, tárolása és megsemmisítése mindig az irányadó elvek szerint történjen, hogy megelőzzük az adatszivárgást vagy adatlopást.

Megoldási javaslatok:

- Papíralapú dokumentumokat soha ne hagyjunk elöl, megsemmisítés esetén használjuk az iratmegsemmisítőt.
- Pendrive-on tárolt adatok előtt titkosítsuk az eszközt, akár a Windows beépített bitlocker programjával.
- Amennyiben eladjuk, elajándékozzuk telefonunkat, tabletünket vagy számítógépünket, minden esetben wipe-oljuk annak tartalmát vagy kérjünk szakértő segítséget.
- A munkahelyi adatainkat soha ne küldjük el privát e-mail-címünkre és ne használjuk az irodán kívül, viszont adatainkról célszerű biztonsági másolatot készíteni.

8. Speciális célszoftverek – OSINT-iparág

Az első programok, amelyek nyílt információkat gyűjtöttek, tulajdonképpen már a digitális hálózatok, majd később az internet szélesebb körben való elterjedésével egyidőben megjelentek, de a kimondottan OSINT-felhasználásra szánt speciális programok a szociális média megjelenésével és elterjedésével kezdtek egyre nagyobb szerepet kapni, és mostanra már egy egész iparág kezd erre ráépülni.

Ma már jó pár olyan speciálisan OSINT-felhasználásra kínált szoftver közül választhatunk, amelyekkel adatokat és információkat gyűjthetünk egyre szélesebb körben. Ezek a cégek saját fejlesztésű szoftvereikkel és különböző keresőmotorok és algoritmusok segítségével gyűjtik le az adatokat, amelyeket azután tovább lehet finomítani, feldolgozni a kívánt cél érdekében. A már említett adatbázis-kiszivárgások kulcsszerepét ezek a vállalatok is felismerték, és sok esetben ezekből az adatbázisokból

is le tudnak gyűjteni információkat, s ennek a tevékenységnek már csak az internetbiztonsági és jogi kérdések, valamint a GDPR megfelelő pontjai szabhatnak határt.

OSINT-jellegű programokat Freeware,[15] azaz ingyenesen használható, illetve előfizetéses vagy egyszeri használatra megvásárolt licencszel is beszerezhetünk. Léteznek olyan programok, amelyeket bootolható operációs[16] rendszerrel tudunk használni; vannak, amelyek már az IT forensic[17] szakterülethez tartoznak, és használhatunk olyan, a rendszerünkre telepített programokat, amelyekből könnyen ki tudjuk exportálni a releváns adatokat további feldolgozás, elemzés céljából, vagy egy jelentés részeként átadni a kérelmező felé. Ezeket a programokat folyamatosan fejleszteniük kell az erre szakosodott cégeknek, hiszen ahonnan az adatokat legyűjtik, azok az adatbázisok, keretprogramok is folyamatosan változnak, vagy a jogi szabályok módosulása miatt, vagy egyszerűen a keretprogramok finomítása, megjelenése vagy új funkciók bevezetése okán.

9. Összefoglalás

Tanulmányom keretében az OSINT jelentőségét, a digitális öntudatosság, az interneten történő felelősségteljes megjelenés fontosságának témakörét jártam körül. Látható, hogy számos valós példa támasztja alá annak kellemetlen következményeit, ha a rólunk szóló információkat akarva vagy akaratlanul, de mindenképpen meggondolatlanul osztjuk meg a közösségimédia-felületeken, de ugyanígy végzetes kihatása lehet annak is, ha jelszavainkat nem kellő körültekintéssel választjuk meg, változtatjuk, illetve tároljuk. Saját magunkon kívül kiemelt figyelmet kíván a legfiatalabb és a legidősebb korosztály felkészítése az online szereplés kockázataira, a veszélyforrások elleni prevenció. A 4. ipari forradalom korát élve az online világban a felhasználókra leselkedő veszélyek napról-napra újabb, változatosabb formában jelennek meg, ami fokozottan hívja fel rájuk a figyelmet és teszi egyben szükségessé e fenyegetettségek folyamatos és hatékony kezelését. Kutatásom keretében éppen ezért számos, nem csak a számítástechnika területén jártas személyek számára könnyen elsajátítható jó gyakorlatot vonultattam fel a kockázatok csökkentése, elkerülése érdekében.

Felhasznált irodalom

Bányász Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe. *Nemzetbiztonsági Szemle,* 3. (2015), 2. 21–36. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1974/1259

Benedek Gergő: *Mi is az az IOT? És mi az AIOT? Minden, amit a dolgok internetéről tudni kell.* (2020. február 12.). Online: https://lexunit.hu/blog/iot/

[15] Anjaneyulu Naini: 8 Popular Open Source Intelligence Tools for Penetration Testing. *Geekflare,* 2021. május 26. Elérhető: https://geekflare.com/osint-tools/

[16] Kali: *The Most Advanced Penetration Testing Distribution:* www.kali.org/

[17] Michael G. Noblett – Mark M. Pollitt – Lawrence A. Presley: Recovering and Examining Computer Forensic Evidence. *Forensic Science Communications,* 2. (2000), 4.

Bodnár Zsolt: Csak kiejted a szádon, hogy „üdítő", és már jön is szembe a neten a kólahirdetés. Mi folyik itt? *Qubit,* 2018. augusztus 21. Online: https://qubit.hu/2018/08/21/csak-kiejted-a-szadon-hogy-udito-es-mar-jon-is-szembe-a-neten-a-kolahirdetes-mi-folyik-itt

Cipriani, Jason: SIM swap fraud: How to prevent your phone number from being stolen. *Cnet,* 2020. szeptember 29. Online: www.cnet.com/how-to/sim-swap-fraud-how-to-prevent-your-phone-number-from-being-stolen/

Davis, Jessica: Hacker Leak COVID-19 Vaccine Data Stolen During EU Regulator Breach. *Health IT Security,* 2021. január 13. Online: https://healthitsecurity.com/news/hackers-leak-covid-19-vaccine-data-stolen-during-eu-regulator-breach

Hurst, Daniel– Lily Kuo – Charlotte Graham-McLay: Zhenhua Data Leak: personal details of millions around world gathered by China tech company. *The Guardian,* 2020. szeptember 14. Online: www.theguardian.com/world/2020/sep/14/zhenhua-data-full-list-leak-database-personal-details-millions-china-tech-company

Lica: Kémprogramokkal ellenőrzik a gyerek netezését. *Index.hu,* 2013. május 5. Online: https://index.hu/tech/2013/05/05/gyerek_internet_biztonsag/

Meyer, Bernard: COMB: largest breach of all time leaked online with 3.2 billion records. *Cybernews,* 2021. február 12. Online: https://cybernews.com/news/largest-compilation-of-emails-and-passwords-leaked-free/

Naini, Anjaneyulu: 8 Popular Open Source Intelligence Tools for Penetration Testing. *Geekflare,* 2021. május 26. Online: https://geekflare.com/osint-tools/

Noblett, Michael G. – Mark M. Pollitt – Lawrence A. Presley*:* Recovering and Examining Computer Forensic Evidence. *Forensic Science Communications,* 2. (2000), 4. Online: https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm

Perei Dóra: Hogyan védekezhetünk a SIM-csere átverés ellen? *Rakéta,* 2021. január 11. Online: https://raketa.hu/hogyan-vedekezhetunk-a-sim-csere-atveres-ellen

Pőcze Balázs: Öt mondatban: mi az a kétfaktoros autentikáció, és miért jó nekem? *Rakéta,* 2019. november 12. Online: https://raketa.hu/ketfaktoros-azonositas

Tips & Tricks – Tech: *Nézd meg az EXIF metaadatokat iPhone, Android, Mac és Windows rendszeren.* (é. n.) Online: http://hu.tipsandtricks.tech/nezd-meg-az-exif-meta-adatokat-iphone-android-mac-es-windows-rendszeren

Jogi forrás

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) *A természetes személyeknek és személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)* (EGT-vonatkozású szöveg). Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016R0679&from=HU